DATE(S) ISSUED:
12/06/2011
12/16/2011 - Updated

SUBJECT:
Vulnerability in Adobe Reader and Acrobat Could Allow For Remote Code Execution (APSB11-04)

ORIGINAL OVERVIEW:
A vulnerability has been discovered in Adobe Reader and Acrobat that could allow an attacker to take control of the affected system. Adobe Reader allows users to view Portable Document Format (PDF) files, while Adobe Acrobat offers users additional features such as the ability to create PDF files. Successful exploitation could result in an attacker gaining the same privileges as the logged on user. Depending on the privileges associated with the user, an attacker could then install programs; view, change, or delete data; or create new accounts with full user rights. Failed exploit attempts will likely cause denial-of-service conditions.

Currently, Adobe has received reports of the vulnerability being actively exploited in the wild in limited, targeted attacks against Adobe Reader 9.x on Microsoft Windows.

An update for Adobe Reader and Acrobat 9.x for Windows will be release no later than the week of December 12, 2011.

December 16 UPDATED OVERVIEW:
Adobe has released an update that addresses this vulnerability for Windows systems only. Adobe is planning to address this vulnerability in Macintosh and UNIX as part of the next quarterly update scheduled for January 10, 2012.

SYSTEMS AFFECTED:
- · Adobe Reader X (10.1.1) and earlier 10.x versions for Windows and Macintosh
- · Adobe Reader 9.4.6 and earlier 9.x versions for Windows, Macintosh and UNIX
- · Adobe Acrobat X (10.1.1) and earlier 10.x versions for Windows and Macintosh
- · Adobe Acrobat 9.4.6 and earlier 9.x versions for Windows and Macintosh

RISK:
Government:
- · Large and medium government entities: **High**
- · Small government entities: **High**

Businesses:
- · Large and medium business entities: **High**
- · Small business entities: **High**

 Home users: High

ORIGINAL DESCRIPTION:
Adobe Reader and Acrobat are prone to a U3D memory corruption vulnerability that could allow an attacker to take control of the affected system. Successful exploitation could result in an attacker gaining the same privileges as the logged on user. Depending on the privileges associated with the user, an attacker could then install programs; view, change, or delete data; or create new accounts with full user rights. Failed exploit attempts will likely cause denial-of-service conditions.

Currently, Adobe has received reports of the vulnerability being actively exploited in the wild in limited, targeted attacks against Adobe Reader 9.x on Microsoft Windows.

An update for Adobe Reader and Acrobat 9.x for Windows will be release no later than the week of December 12, 2011.

Adobe Reader X Protected Mode and Adobe Acrobat X Protected View will prevent an exploit of this kind from executing. Adobe will not be releasing an update for Adobe Reader X and Adobe Acrobat X for Windows until January 2012. To verify Protected View for Acrobat X is enabled, go to: Edit >Preferences> Security (Enhanced) and ensure "Files from potentially unsafe locations" or "All files" with "Enable Enhanced Security" are checked. To verify Protected Mode for Adobe Reader X is enabled, go to:Edit >Preferences >General and verify that "Enable Protected Mode at startup" is checked.

December 16 UPDATED DESCRIPTION:
Adobe has released an update that addresses this vulnerability for Windows systems only. Adobe is planning to address this vulnerability in Macintosh and UNIX as part of the next quarterly update scheduled for January 10, 2012.

ORIGINAL RECOMMENDATIONS:
The following actions should be taken:
- Install the updates provided by Adobe as soon as they are made available after appropriate testing.
- Run all software as a non-privileged user (one without administrative privileges) to diminish the effects of a successful attack.
- Consider installing and running Adobe Reader X in Protected Mode.
- Remind users not to visit untrusted websites or follow links provided by unknown or untrusted sources.
- Do not open email attachments from unknown or untrusted sources.

December 16 UPDATED RECOMMENDATIONS:
The following actions should be taken:
- Users of Adobe Reader 9.4.6 and earlier 9.x versions for Windows update to Adobe Reader 9.4.7.
- Users of Adobe Acrobat 9.4.6 and earlier 9.x versions for Windows update to Adobe Acrobat 9.4.7.

ORIGINAL REFERENCES:

Adobe:
http://www.adobe.com/support/security/advisories/apsa11-04.html
http://blogs.adobe.com/asset/2011/12/background-on-cve-2011-2462.html

CVE:
http://cve.itre.org/cgi-bin/cvename.cgi?name=CVE-2011-2462

December 16 UPDATED REFERENCES:

Adobe:
www.adobe.com/support/security/bulletins/apsb11-30.html

CVE:
http://cve.itre.org/cgi-bin/cvename.cgi?name=CVE-2011-4369